NOTICE OF EX PARTE

September 23rd, 2015

VIA ECFS

Re: *Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment (ET Docket No. 15-170).*

On September 21st, the FCC hosted a phone conference to discuss Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment (ET Docket No. 15-170, herein referred to as "proposed rules"). Pursuant to Section 1.1206 of the Commission's rules, the following document contains a summary of oral ex parte presentations made by Joshua Gay of the Free Software Foundation (FSF). In accordance with Section 1.1206(b) of the Commission's rules, documents shown or given to Commission staff during ex parte meetings are deemed to be written ex parte presentations. The Appendix of this filing contains questions and comments provided to the FCC by the FSF in advance of and during this meeting. The Appendix formed the basis for much of the conversation.

The following individuals from the FCC attended part or all of the meeting:

- Brian Butler
- Rashmi Doshi
- Nicholas Oros
- Jamison Prime
- Bruce Romano
- James Szeliga
- George Tannahill

The following individuals from the FSF attended part or all of the meeting:

- Joshua Gay
- John Sullivan

Statements made by the FSF

In addition to briefly stepping through all of the document presented in the Appendix to this document, the FSF also raised the following concerns regarding the proposed rules.

- The FSF is concerned that the proposed rules would result in authorized equipment in which the end user would not be able to control the device or be able to install software on their device.

- Further, due to the design of most modern hardware produced today, the majority of authorized equipment would not have a clear separation between the software that controls the radio and other functionality that the software could potentially provide (such as having access to user's data and the ability to control the CPU of the device and the ability to transmit that information with or without the consent or knowledge of the

owner of the device).

- In addition, since the proposed rules would require a user to give-up control of the part of the device that can control radio communication and thus they would be granting absolute and exclusive control to "authorized parties" to determine how, what, and where the radio will communicate and operate. This means that user's would be giving up all control and they have no reason to trust the authorized parties. Given that it is common for manufacturers to distribute faulty software or software with security flaws, the proposed rules would by design, prevent the user/owner of a device from being able to fix certain security flaws.
- Lastly, the FSF raised the point that the proposed rules could create vendor lock-in on software for hardware devices and this creates an unfair advantage for manufacturers who have FCC approval on the device, since they have no incentive to provide software updates on the devices that are certified, when they can simply require users to purchase new hardware equipment that comes with updated software.

Statements form the FCC

The following is a summary of responses and statements made by the FCC in response to the questions and concerns raised by Joshua Gay of the FSF:

- The FCC affirmed that the proposed rules would prevent user's from making changes to the software, even if that software complied fully with the Commission's rules.
- The FCC stated that scope of the proposed rules in question only extends to the software which controls the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates according to the Commission's rules.
- The FCC explained that in 2014, 47 CFR 15.407 was updated to included rules that would require manufacturers to put in place mechanisms that would restrict a user's ability to control or modify the software that controls the radio. The following text from 47 CFR 15.407 was referenced:
- "All U-NII devices must contain security features to protect against modification of software by unauthorized parties."
- "Manufacturers must implement security features in any digitally modulated devices capable of operating in any of the U-NII bands, so that third parties are not able to reprogram the device to operate outside the parameters for which the device was certified. The software must prevent the user from operating the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved for the device."
- The FCC stated that the they do not believe that the proposed rules would prevent a person from bringing an FCC authorized device outside of the country and installing software changes that would permit the device to operate according to the rules of

another legal jurisdiction.

Appendix

In accordance with Section 1.1206(b) of the Commission's rules, the following contains an exact copy of statements and questions presented to the FCC by the FSF in advance of the above referenced meeting.

The FSF is a 501(c)3 charitable corporation with its main offices in Boston, Massachusetts. The FSF believes that people should be free to study, share and improve all the software they use and that this right is an essential freedom for users of computing. The FSF has been working to achieve this goal since 1985 by directly developing and distributing, and by helping others to develop and distribute, software that is licensed on terms that permit all users to copy, modify and redistribute the works, so long as they give others the same freedoms to use, modify and redistribute in turn. The FSF is the largest single contributor to the GNU operating system (used widely today in its GNU/Linux).

The FSF thanks the Commission and the Office of Engineering Technology for agreeing to meet with the FSF to discuss the Notice of Proposed Rule Making (rel. July 21, 2015), which proposes substantial updates to Commission's Rules regarding authorization of radiofrequency equipment.

It is the FSF's understanding that nearly all new consumer wireless devices sold in the United States will be effected by this NPRM. The FSF's first concern with computer hardware devices is whether a user will have the ability to install and run free software on their devices. When we speak of "user" in this context, it includes not only an individual user, but also schools, hospitals, government agencies, and myriad other institutions that wish to be able to modify and control their wireless hardware devices and wireless communications infrastructure.

With this in mind, we humbly submit the following questions.

Question 1

The NPRM states: "(i) For devices including modular transmitters which are software defined radios and use software to control the radio or other parameters subject to the Commission's rules, the description must include details of the equipment's capabilities for software modification and upgradeability, including all frequency bands, power levels, modulation types, or other modes of operation for which the device is designed to operate, whether or not the device will be initially marketed with all modes enabled. The description must state which parties will be authorized to make software changes (e.g., the grantee, wireless service providers, other authorized parties) and the software controls that are provided to prevent unauthorized parties from enabling different modes of operation. Manufacturers must describe the methods used in the device to secure the software in their application for equipment authorization and must include a high level operational description or flow diagram of the software that controls the radio frequency operating parameters. The applicant must provide an attestation that only permissible modes of operation may be selected by a user."

Many wifi chipsets are designed to operate in different ways depending on the legal jurisdiction (region) in which the device is located. This region information is often set by the operating system of a wireless device. A user is able to install custom versions of an operating system and in doing so, they are able to set the region information however they wish, and therefore, potentially enable different modes of operation of the wireless device.

Is it the intent of the above proposed rule to no longer certify devices that make use of region information set in the operating system, including the Linux kernel and Linux kernel drivers, if doing so would allow the device operate in non-permissible modes of operation?

Question 2

Where the NPRM states: "The description must state which parties will be authorized to make software changes (e.g., the grantee, wireless service providers, other authorized parties) and the software controls that are provided to prevent unauthorized parties from enabling different modes of operation."

Is the intent of this language, that in general, the user and owner of a device will not be allowed or considered to be an authorized party to make changes to the software?

Question 3

For many devices, which would qualify as certified modular transmitters, the only way of installing new system software on the device is to "reflash" the entire system with new software. The proposed rules pertaining to certified modular transmitters that use software defined radios, state: "Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements."

Laptops, single board computers, and many other computing devices appear to fall under the category of certified modular transmitter. Is it the intent of the commission to not allow a user to install their own custom versions of the system software if that software could in some way control the operating of the radio device in non-permissible ways?

Question 4

In many computer systems, there exists system software (such as UEFI) that manages signature checking of various system firmware. If such systems are used for the electronic signature checking of wireless chipset firmware, does this mean that a user would not be able to turn off electronic signature checking functionality if doing so would permit the installation of non-authorized firmware?